The Information Commissioner's Office's response to a Call for Evidence from the Secretary of State for the Department for Digital, Culture, Media and Sport on the National Data Strategy

The Information Commissioner has responsibility for promoting and enforcing the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR); the Privacy and Electronic Communications Regulations 2003 (PECR); the INSPIRE Regulations; eIDAS Regulations; Re-use of Public Sector Information Regulations; and the NIS Regulations.

The Information Commissioner is independent of Government and upholds information rights in the public interest, promoting transparency and accountability by public bodies and organisations and protecting individuals' privacy and information access rights.

The Information Commissioner's Office (ICO) welcomes the Government's intention to develop a National Data Strategy and the opportunity to respond to the open call for evidence.

The digital revolution offers a multitude of benefits and opportunities – from economic growth and technological innovation to the delivery of more efficient and tailored public services. The Call for Evidence rightly identifies big data – much of it personal data - as the fuel driving the digital economy. But in order for the value of Big Data to be fully realised, citizens need to have trust and confidence in how that data is being used.

Innovation in the digital economy relies on the trust of consumers to generate the social licence that companies need to break new frontiers with data. Growth built on a healthy foundation of trust is sustainable. Growth built on mistrust is vulnerable to the reputational damage of a data breach.

Effective, modern data protection laws with robust safeguards are central to securing the public's trust and confidence in the use of personal information within the digital economy, the delivery of public services and the fight against crime.

The GDPR puts an increased onus on organisations to take a proactive approach to data protection, identifying the risks they are creating

through their use of data, and working to reduce and mitigate those risks. The greater enforcement powers granted to the ICO has helped to establish compliance as a board-level issue. Privacy and innovation need to work hand in hand in today's evolving digital economy.

The attached response is divided into a number of key headings, which aim to cover the broad spectrum of objective and questions in the Call for Evidence, with a focus on providing relevant evidence from an information rights regulatory and legislative perspective.

The three key strands that run through our response are; *accountability, transparency and trust.* These principles should be at the heart of the proposed National Data Strategy. Personalisation is a powerful tool in the development of the digital economy. It is therefore essential that data protection principles and legislation are a central pillar of the Strategy. Our response includes evidence of the impact of the GDPR and DPA18 on accountability, transparency and trust after one year on from implementation; and practical examples of what businesses and organisations can do to demonstrate how these principles are embedded in their business models so that society is able to fully realise the economic, educational and social benefits of the digital revolution.

Although the Strategy will be primarily focused on unlocking the power of data to support the UK build a world leading digital economy, we also think the Strategy needs to emphasise the importance of openness of information and accountable decision-making in how decisions are made by public services and institutions and why. In this sense, data protection and freedom of information law are two sides of the same coin. They enable individuals to probe, challenge and access decisions that impact on them and their lives. Both laws are key tools for democracy, citizen engagement and a flourishing digital economy. Our submission therefore makes reference to some of our current work and thinking in this area. Finally, we would recommend that the Government considers how the Strategy will fit with other related initiatives at an international, devolved and local level – to take advantage of synergies and opportunities for collaboration and avoid duplication.

The ICO is committed to supporting the Government in the development of a National Data Strategy and looks forward to discussing the content of this submission further.

Introduction

This response reflects two of the areas of information rights that the ICO regulates, namely data protection and freedom of information. Data protection is a particular focus because of the new legislation that came into effect in 2018.

People

Trust

(Questions 1.1, 1.2, 1.3, 1.5, 1.6, 1.8, 1.9, 2.1)

1. People want access to products and services, but they also want to know how and why their data will be used. They want their privacy to be respected, so that if their data is processed or shared, they can be assured that it will be used responsibly and kept securely. If organisations can show them that their data is responsibly used and kept securely, people are more likely to trust them with their data.

2. The accountability and fairness principles in GDPR place a responsibility on organisations, including Government, to understand the risks that they create for others with their data processing, and to mitigate those risks. Data protection needs to be part of the cultural and business fabric of any organisation processing personal data.

3. Accountability provides an opportunity for organisations to show, and prove, how they respect people's privacy rights, which helps to develop and sustain people's trust. It is no longer sufficient just to comply with the law. Organisations need to actively demonstrate their compliance by embedding privacy principles into their systems and processes and manage risk. To this extent, data protection is now a board-room issue.

   What people and organisations are telling the ICO

4. As the UK's information rights regulator, the ICO has continued to receive an increased number of complaints in all areas of its remit, since May 2018[1]. For example, in 2018-19, we received 41,661 data protection complaints from the public, compared with 21,019 in 2017-18.

5. We also received 138,368 complaints under PECR in 2018-19 (up from 109,481 in 2017-18). These included complaints about telesales calls and spam texts.

[1] https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf

6. These statistics suggest that there is:

    - greater awareness of information rights and of the new data protection legislation, since the advent of the GDPR; and
    - greater awareness of the ICO as the information rights regulator.

7. This is also borne out by our survey of data protection officers in March 2019, when 64% stated that they either agreed or strongly agreed with the statement "I have seen an increase in customers and service users exercising their information rights since 25 May 2018."

8. GDPR and the DPA strengthened the requirement for organisations to report personal data breaches, and these also increased, rising from 3,311 in 2017-18 to 13,840 in 2018-19.

9. The change in the regulatory landscape has shown the importance of getting privacy right. People have woken up to the new rights the GDPR delivers, with increased protection for the public and increased obligations for organisations. But there is much more still to do to build the public's trust and confidence. With the initial hard work of preparing for and implementing the GDPR behind us, there are ongoing challenges of operationalising and normalising the new regime. This is true for businesses and organisations of all sizes. The ICO is committed to supporting DPOs and organisations to get things right. We celebrate and champion excellence in the data protection field. For those who do not take this responsibility seriously or those who break the law, we will act swiftly and effectively.

10. We recommend that the National Data Strategy emphasises the importance of taking appropriate measures to meet the requirements of the accountability principle and of adopting a data protection by "design and default" approach as part of an organisation's compliance with the data protection legislation.

    Opportunities for greater trust through accountability and transparency

11. Organisations are responsible for complying with the GDPR and must be able to demonstrate their compliance. They need to put in place appropriate technical and organisational measures to meet

the requirements of accountability.[2] In particular, we recommend Data Protection Impact Assessments (DPIAs) as a way to build trust and confidence with individuals and the wider public. Organisations need to carry out DPIAs[3] for processing that is likely to result in high risk to individuals. A robust DPIA will ensure that an active focus is placed on individuals' information rights when processing data. The Government may want to consider including requirements for DPIAs to be published (in a redacted or extracted form, if necessary) as it is a good way to demonstrate accountability and transparency.

12. To assist data controllers in meeting their responsibilities under the accountability principle, we are in the early stages of developing an accountability framework that organisations will be able to use to help check they meet our expectations in this area. We expect to have a framework available for organisations to use early in 2020. The Government may wish to consider including a reference to this in the National Data Strategy.

Enhancing trust through transparency

13. Individuals have the right to be informed[4] about what personal data is collected, why it is being used and who it is shared with, amongst other information. They have a range of additional rights[5], including a right of access to their own personal data to see what information an organisation holds about them, and how that data is being used.

14. The GDPR also contains the right to erasure also known as the right to be forgotten. Given the prevalence of individuals posting images and information online, this particular right is likely to become of increasing relevance. For example, many parents post images of their children on social media and the right to be forgotten may become particularly important as these digital natives grow up.

15. The public is concerned:

    - about who their data is shared with; and
    - that they have lost control over how their data is used.

    So it is important that any Government ambitions to make better use of data and to maximise the use of data analytics and artificial

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

[3] Organisations may also need to formally consult with the ICO on their DPIA in certain circumstances – see Article 36 GDPR

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

intelligence (AI) inspire confidence in data subjects. The role of the Commissioner as an independent regulator continues to play an important part in helping to build the public's trust and confidence in the use of their data.

16. We provide guidance about the information that data controllers should include in privacy policies[6] which should be concise, transparent, intelligible, easily accessible and in clear language. These need to include:

    - all the purposes of the processing including what happens beyond the initial collection of data;
    - how and with whom the controller may be sharing the data;
    - how long the controller will hold the data, including how many times it might be re-used and circulated; and
    - whether the controller will aggregate the data with other information, which will then be used for, for example, profiling and marketing.

17. We also recommend that the National Data Strategy sets data standards which will apply across Government (and any other sectors that the Strategy might cover) to reduce the potential adverse impact of differences in practice. This is in the light of our experience that different systems and data inputting protocols can adversely impact individuals. For example, the shortening of a name or a variation in spelling might lead to an individual believing they have exercised their right to be forgotten, but the data remains.

Barriers to trust – our priority investigations

18. We have launched a number of 'own motion' investigations[7], which help the public to become more aware of how their data is being used. These allow us, for example, to highlight and address otherwise opaque or 'invisible' processing of personal information. We have used these 'own motion' investigations to look into data protection practices which concern us as a regulator, but which have not yet been the subject of significant public complaints. For example, our investigation into the use of personal data for targeted advertising[8] was aimed at 'pulling back the curtain' on areas where there may have been 'invisible' processing.

[6] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/
[7] https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf
[8] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/

19. Our priority investigations have resulted in the ICO issuing enforcement notices[9], compelling the controller in question to comply with data protection laws within a specified time. Our enforcement action has underlined that while, for example, new technologies, including biometric technology, can bring substantial benefits to organisations and the public, they must be used appropriately and in a way that the public can be clear and confident about[10].

20. We also took enforcement action as part of our investigation into the use of data analytics in political campaigns and published 'Democracy Disrupted[11]', our policy report. One of our key recommendations was the need for a statutory code of practice on the use of personal data in political campaigns. Through the other recommendations, we sought to improve transparency and protect personal data and information rights in political campaigning.

21. Our continuing investigation into the use of victims' data aims to identify how data of complainants is processed through the criminal justice system in cases where rape and serious sexual offences are being investigated. Many of the concerns and issues raised in this case are also shared with the ICO's continuing high priority investigation into the use of mobile phone extraction for policing purposes. The most central issue arising in both cases is the requirement to maintain and enhance public confidence in how personal data is used in police investigations.

22. Processing of special category data, and particularly health data, is often of most concern to individuals. Use of biometric data (for example, in facial recognition technology) is also a concern if introduced without proper safeguards. In another of our high profile investigations, we have highlighted our concerns about the potential for misuse of facial recognition technology and the need to ensure data protection law is adhered to when using it. Our investigations seek to shape our response to the emerging use of this technology by a large number of law enforcement, public sector and private sector bodies.

Inclusivity
(Questions 2.3, 2.4, 2.5)

[9]For example, an enforcement notice was issued in respect of the Metropolitan Police's 'Gang Matrix' – see https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf
[10] For details of the enforcement notice issued in respect of HMRC's Voice ID service, see https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf
[11] https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

23. We have not undertaken research to establish whether participation in data differs by sector but, anecdotally, we see more innovation in the use of personal data in certain sectors, such as the financial sector. We are also aware that there is some SME activity in this sector. There is also evidence of innovation in the healthcare sector but particular care is needed when processing special category data, as well the need to take into account the importance that individuals attach to their health information.

24. Data protection legislation protects individuals' personal data rights. When personal data is lost, stolen or shared or used inappropriately it can lead to harm, distress and negative impacts on personal rights and freedoms. This means that data protection measures are especially important for processing which involves vulnerable individuals and families, including victims of domestic abuse and victims of crime.

25. Similarly, we are aware that certain sectors of society can be disadvantaged because of a lack of data literacy or personal circumstances. These groups can include the sick and infirm, the elderly, those without access to the internet or who lack the skills or literacy to use it, those whose first language is not English, and those who are disadvantaged because of their personal circumstances, such as poverty and homelessness. Many may be socially disadvantaged and may have particular need of the services provided by Government, such as Universal Credit. And yet, for example, some homeless people may not have bank accounts, or evidence to establish their identity to allow them to establish links with their service providers. The risk of exclusion of these communities is great and care needs to be taken to given them control and agency over their own data.

26. As part of our grants programme, the ICO has granted funding to Connection[12], a charity for the homeless, in a project to explore awareness of information rights in the homeless community. Although the project is at an early stage, it is hoped that it will produce evidence about some of the barriers faced by this community in the use of their data and the exercise of their information rights.

Children

27. The GDPR states that children merit special protection[13] and specific care should be taken to ensure that the privacy information

[12] https://www.connection-at-stmartins.org.uk/
[13] Recital 38 GDPR

provided to the children involved is clear, in plain language and understandable by the child.

28. Children's privacy is a key area of regulatory risk and a priority for the ICO. We are presently developing our Age Appropriate Design Code of Practice[14] which draws on additional research commissioned by the ICO. The draft Code sets down standards for information society services to follow and practical guidance on how to design data protection safeguards into online services to ensure they are appropriate for use by, and meet the development needs of children.

29. The draft Age Appropriate Design Code recognises that marketing and strategies used to extend user engagement can potentially be detrimental to children. This can include issues of trust, but the impacts may be wider, for example on physical or mental health. The code states that organisations should not process personal data in ways that have been shown to be detrimental to children or that go against industry standards, regulatory requirements or Government advice. We are presently considering the responses we received to the public consultation on this Code.

30. The ICO has funded a project (as part of its grants programme) with the London School of Economics into children's information rights and privacy, particularly with regard to children's capacity to consent and the production of an accessible online toolkit for children, parents and teachers. This research indicated that, although children may be aware of their personal social privacy, they are less aware of the extent to which organisations share their data. This links in with the discussions elsewhere in this response regarding the importance of transparency and the responsibility on organisations to be accountable for the way that they use data.

Summary on inclusivity

31. Our work on data protection in relation to disadvantaged or vulnerable groups is evolving. However, a central point that we recommend for inclusion in the National Data Strategy is that, in their efforts to deliver better outcomes for vulnerable individuals, organisations need to ensure that they do not overlook the importance of the individual's privacy rights. We would also recommend that the National Data Strategy places prominence on the need to take account of the particular risks and responsibilities that arise when processing children's data and that it makes explicit

[14] This Code is still in draft form, following public consultation https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf

reference to the need to follow the Age Appropriate Design Code, which is due to be published later this year.

32. We also acknowledge the significant role that civil society groups play in raising issues and holding organisations to account, particularly amongst disadvantaged groups. The ICO has itself responded to the need for public awareness by developing a range of materials aimed at helping individuals to exercise their rights and explain how their information is used. For example, guidance such as Your Data Matters (YDM)[15] which explains information rights, including what organisations should explain proactively and the rights of access and objection. The YDM campaign gained extra reach because it was developed and rolled out in collaboration with a range of high profile organisations in the public and private sector, including banks, retailers and the NHS. This is an approach that might be helpful when developing the National Data Strategy.

Data skills and employment
(Questions 2.6, 2.7 and 2.9)

33. It is important that organisations provide all employees and other workers with information rights training – including FOI training and data protection training that is appropriate to their role - to ensure that their employer can comply with their obligations under the law.

34. Growing information rights skills is key to embedding accountability as part of a culture change, and organisations need to provide sufficient board level commitment to secure adequate resources and support for data protection measures. Data protection officers (DPOs) play a key role in this, by monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding DPIAs and acting as a contact point for data subjects and the supervisory authority. Their independence and expertise in data protection must be adequately resourced, and they need to report to the highest management level. DPOs can help organisations demonstrate compliance and are part of the enhanced focus on accountability.

35. It's also vital to embed concepts such as data protection by design and default in an organisation's culture. This requires appropriate levels of knowledge of data protection law on the part of system designers, builders and programmers to ensure that risks can be identified and addressed or mitigated as they arise in the lifetime of a project.

[15] https://ico.org.uk/your-data-matters/

36. The ICO supports the public directly through our many expanded public-facing services (like our helpline and live text service), as well as providing organisations with indirect support through the various tools it has made available for companies, small or large, to explain the new laws and rights.[16]

37. In addition, the ICO has developed materials for schools to help teachers to include content on privacy and data protection in lessons[17]. We have also funded work to develop materials to embed in higher education courses to grow data protection capability in the workforce.

38. The ICO also currently has a grants programme[18] which is presently supporting innovative research into privacy enhancing solutions.

39. The National Data Strategy provides an opportunity for Government to consider expanding on the growth of information skills and growing data protection capability in the education system. Employability is key for the education sector and data protection is ever more important given aspects such as mass data capture, personalisation, and information rights which are still relatively poorly understood in the population as a whole. At an individual level, investment in these areas will link to digital literacy.

40. We would also like to see steps being taken in Government policy to enhance inclusion in respect of information rights, through greater consultation with the public on the part of the sectors included in the Strategy. This would present opportunities to educate the public about what is happening to their information and the potential consequences for them. We have done this as part of our work on developing the Age Appropriate Design Code, seeking views from children as well as parents and carers. In other areas, we have used citizens' juries as a useful tool for explaining complex concepts and enabling people to express a more informed opinion.

Economy

Operating in a data driven economy

[16] https://ico.org.uk/

[17] See for example https://icosearch.ico.org.uk/s/redirect?collection=ico-meta&url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DxtLR0Ey5-vo%26feature%3Dyoutube_gdata_player&index_url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DxtLR0Ey5-vo%26feature%3Dyoutube_gdata_player&auth=LICdI6q0hw5tXi%2F1rk2ikQ&profile=_default&rank=5&query=schools-

[18] https://ico.org.uk/about-the-ico/what-we-do/grants-programme-2018/

(Questions 1.2, 1.3, 1.5 1.7, 3.1, 3.2, 3.3, 3.4, 3.6, 4.3)

41. Our research in July 2018[19] found that one in three (34%) people have high trust and confidence in companies and organisations storing and using their personal information – significantly up from the 21% stating this in 2017. This is a welcome rise, which could be attributed to GDPR and DPA 2018. This data is, of course, now a year old, and was obtained when GDPR had only just been introduced. Further research will be needed over time to assess this and we will be conducting a further survey in July 2019.

42. Businesses that do not respect privacy and data protection will ultimately find that the public lose trust in them; being privacy friendly and compliant with data protection law will be a competitive advantage in the long run[20].

43. Virtually all businesses nowadays rely on personal data to a greater or lesser extent for their business models to work, given the significant focus on personalisation. It might also be argued that personal data is, in many circumstances, still perceived as a resource to be exploited rather than a protected asset. The often-used quote that "data is the new oil" holds significant currency.

44. Many large technology firms make money through the use of personal data.[21]They rely on advertising revenue for their commercial success, driving the need for maximum and sustained user engagement. This results in more personal data, data acquisition, profiling and user manipulation. Marketing more generally is one of the principal ways through which companies are seeking to monetise personal data.

45. Companies also make money through personal data via database checking services (for example, credit reference agencies, screening services), surveillance technologies (CCTV, facial recognition, automatic number plate recognition (ANPR)), in financial services and insurance, in healthcare, and in many other sectors.

46. New and innovative ways of processing personal data, as well as increased portability of personal data under GDPR can provide new opportunities for organisations and businesses to provide improved products and services for individuals. However they also bring new risks which it is essential to address and mitigate.

[19] https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf
[20] See also our comments under the Trust section above
[21] https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

47. Organisations such as the Centre for Humane Technology[22] actively support individual and collective wellbeing online, and provide self-help tools. But data protection regulation has to be seen as part of the wider ecosystem of regulating the internet and should not be positioned separately. We refer to the Commissioner's response to the Government's Online Harms White Paper[23] regarding the risks that increased personalisation of online content creates for society and how they might be addressed.

48. New enforcement powers in GDPR and DPA 2018 have significantly strengthened the ICO's hand and focused minds on the importance of making data protection a board-room issue at most organisations.

49. Accountability under GDPR ensures business can:

    - demonstrate compliance to business partners and regulators;
    - build trust and support data sharing; and
    - help mitigate enforcement action and reputational damage when things go wrong.

    Accountability also offers a competitive edge, because it is an opportunity to prove that people's privacy is respected, and this builds trust.

50. Key components of accountability are scalability and risk assessment, which help businesses prioritise data protection, implement proportionate measures, and enable organisations to engage in more complex data processing such as AI and machine learning.

51. But it is also essential that Government builds privacy into the development of public policy, ensuring that individuals' fundamental privacy rights are central to the National Data Strategy. We refer to the Commissioner's response to the Digital Competition Expert Panel's independent review consultation on 'The State of Competition in the Digital Economy[24].

Competition: small/medium businesses
(Questions 3.1, 3.2, 3.3, 3.4, 4.1, 4.2, 4.7)

[22] https://humanetech.com/
[23] https://ico.org.uk/media/about-the-ico/consultation-responses/2019/2615232/ico-response-online-harms-20190701.pdf
[24] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785549/DCEP_Public_responses_to_call_for_evidence_from_organisations.pdf

52. We recognise that it hasn't been easy for small organisations, and particularly sole traders, to become compliant with GDPR and DPA[25]. Concepts such as legal bases for processing, data auditing and privacy policies take time to understand and there are no quick fixes for making sure people's personal data is being processed legally.

53. It may be more difficult for smaller organisations to understand their data protection obligations and put in place the required measures to demonstrate their accountability. The nature of the processing and level of risk will affect what is required.[26] This may also be more challenging if they are processing personal data of a complex nature or which is in a greater risk category.

54. To help this community understand its data protection responsibilities, the ICO has provided a suite of resources, support and guidance on our website, tailored to the needs of sole traders and small organisations[27]. The ICO is also planning to create a dedicated team to support them.

55. We know that many small businesses are involved in innovative projects in sectors like Fintech. Many use services provided by larger organisations (e.g. Cloud Computing services) which invert the usual controller relationship as the power rests with the service provider. Large companies can use this as a selling point to help smaller organisations meet their obligations. However, they need to ensure that their own services are compliant because others rely on them. The National Data Strategy will need to bear in mind the impact of such imbalance of power in its proposals.

56. One of the benefits of increased transparency through stronger information access laws (as recommended in our *Outsourcing Oversight?* report[28]) is that it can help to increase competition by making more information available via the freedom of information regime, and help to level the playing field for SMEs and third sector organisations.

Technological developments and productivity - what does the public know about how their data is used in innovative areas[29]?

[25] https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf
[26] Accountability and governance – see https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
[27] https://ico.org.uk/for-organisations/in-your-sector/business/
[28] https://ico.org.uk/media/about-the-ico/documents/2614204/outsourcing-oversight-ico-report-to-parliament.pdf
[29] Our comments in this section are also relevant to the section on Trust

57. We have undertaken our own research with citizens' juries with the Alan Turing Institute.[30] This research shows an initial low level of public awareness, although public views are nuanced. Some prioritise system accuracy and performance over 'explainability' - an aspect of transparency - in some contexts but not in others.

58. We recognise that it can be difficult to understand how data is used in AI decisions. This can be due to uncertainty on the part of business about how the legislation should be interpreted but is also partly to do with the technical complexity of the systems. Explaining AI decisions is part of the responsibility placed on organisations who need to build in the necessary controls and contribute to public awareness. Privacy and innovation need to go hand in hand, and the ICO's Project ExplAIn is focused on supporting organisations in this area by producing guidance on explainability of AI decisions.

Technological developments and productivity - Adtech, Real Time Bidding and Cyber Security[31]

59. The ICO commissioned research from Harris Interactive, with advice from OfCom [32] which looked into the adtech industry and its handling of data protection. This research concluded that information was often not understood or people did not feel able to engage with it. When they were shown an explanation of adtech, they shift towards the view that websites that show adverts are unacceptable. Our research showed that the adtech industry still needs to provide assurances that any onward transfers of data will be secure.

60. In other ICO research[33], technologies and practices used in programmatic advertising (known as Real-Time Bidding (RTB)) were investigated. This research also raised concerns about transparency and consent as well as the reliance on contractual agreements to protect how bid request data is shared, secured and deleted. While many RTB market participants place some controls on their processing and sharing of personal data, it has become apparent during our work that there are substantially different levels of engagement and understanding of how data protection law applies and in respect of the issues that arise.

[30] *Project ExplAIn* interim report

[31] Our comments in this section are also relevant to the section on Trust

[32] https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf

[33] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/

61. At a wider societal level, the impact of wide personal data capture and innovative and ever more connected processing on concepts like self-definition and autonomy is even less well understood by the general public. This is despite the possibility that AI and other technology may significantly impact on life issues such as job applications and applications for loans.

62. We already have existing, comprehensive guidance in this area, which applies to RTB and adtech in the same way it does to other types of processing – particularly in respect of consent, data protection by design and DPIAs. We intend on continuing to gather information and engage with the industry to further enhance our knowledge. We'll also continue to share knowledge with our European colleagues. We plan to review our position towards the end of 2019, when we will consider whether our concerns still hold and evaluate whether further action is required.

63. Problems with cyber-security were at the heart of some of the biggest personal data breaches that we investigated in the past year. Three of the major fines we issued (those assessed against Uber, Yahoo! and Equifax) were as a result of failures in cyber security. Other major ongoing investigations under GDPR and DPA have also been related to major cyber security failures. The scale of such breaches and the impact on individuals caused by such events underline the importance of regular security reviews and upgrades to provide resilience against changing threats. The National Data Strategy should place strong emphasis on the necessary technological and organisational measures that are needed to protect data and keep it secure.

Challenges in innovative technologies and uses of data – action we've taken

64. The Commissioner takes enforcement action when it is proportionate and appropriate to do so. For example, an enforcement notice was issued in May 2018 against SCL Elections Limited (Cambridge Analytica) about the misuse of data which was then used on both sides in the UK referendum on membership of the EU[34]. We also imposed a fine on Facebook for its unfair processing of personal data and its failures to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data.[35] The ICO will continue to hold tech firms to account for how they handle citizens' data online.

[34] https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf
[35] https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf

Codes of conduct and certification schemes

65. The ICO have recently launched webpages, inviting organisations to engage in relation to codes of conduct and certification schemes. We would welcome a reference in the National Data Strategy to the assistance that these codes and schemes can offer organisations in evidencing their accountability.

Innovation spaces

66. Drawing on the experiences of the Financial Conduct Authority Sandbox, the ICO has introduced a Sandbox service to support organisations which are developing products and services that use personal data in innovative ways with a clear public benefit. We recently accepted the first entrants into the Sandbox, from a range of organisations.[36] Participants are able to draw on the ICO's expertise and advice on data protection by design, mitigating any risks as they test their innovations, while ensuring that appropriate protections and safeguards are in place.

67. Privacy and innovation are not mutually exclusive and there is no need for an either/or choice between the two. The Sandbox demonstrates the ICO's support for innovation in technology and exciting new uses of data, while ensuring that people's privacy and legal rights are protected. Although more information about the outcome of this work will emerge in due course, we consider that 'sandboxes' or pilot schemes in controlled circumstances are likely to encourage innovation in supportive ways for organisations of all sizes.

68. The ICO's Regulators Business, Innovation and Privacy Hub[37] is helping remove perceived data protection barriers to innovation and developing the capacity of other regulators to address data protection issues. In turn, this assists organisations with demonstrating their accountability under GDPR.

69. We recognise that the data landscape is continually changing. For example, the concept of data trusts are emerging as a way that data can be shared, although more needs to be done to clarify how they might operate in the context of data protection legislation. It would be helpful if the National Data Strategy allowed some

[36] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-selects-first-participants-for-data-protection-sandbox/
[37] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/new-ico-hub-to-support-innovation/

flexibility to ensure that it can be supportive of innovative ideas about the use and sharing of data in ways that preserve information rights and protections.

Summary

70. Data protection is not intended to prevent data being used for good and we recognise the many benefits that can flow from the use of innovative techniques, for individuals, for organisations and for society in general. But these benefits will only truly be felt when privacy rights and data protection are embedded in organisations processing the data. Failing to do so will result in public loss of trust and confidence.

71. Innovative developments present a challenge to the regulator, as there is growing opacity of processing. There is also a challenge to organisations, which need to build trust, particularly when embracing new technologies or new ways of using data, frequently in a fast paced environment. The analysis of big data using techniques made possible by AI has data protection implications, and it can be more challenging to apply the data protection principles when using personal data in a big data context[38].

72. We therefore recommend that particular attention is given in the National Data Strategy to the importance of transparency and accountability, and of explaining and raising awareness about how data is used, especially for processing involving AI and other innovative techniques[39].

Government
(Questions 4.9, 5.2, 5.6, 6.1, 6.4 and 6.6)

Current use of data - the open data agenda, FOIA and EIR

73. The principles of FOIA and EIR promote transparency and accountability in the public sector. These laws equip citizens, the media, advocacy groups and others with information through which they can scrutinize decisions and actions taken by public authorities at all levels. Accountability by the public sector helps it to demonstrate it is worthy of the trust of the people it serves.

74. Access to information in the public interest may secure service improvements that provide the public with lasting benefits. It is used by the public, campaign groups, businesses, the media and

[38] *Big data, artificial intelligence, machine learning and data protection*
[39] See also our response under the Trust section

MPs to shine a spotlight on the public sector, for instance leading to actions that reduce waste or highlighting unfairness.

75. The National Data Strategy is an opportunity to encourage a proactive open data agenda, and support Government in making key changes. The privacy rights of individuals need to be protected in relation to their personal data. But data protection legislation should not be seen as a barrier to the open data agenda, although it does require a proper and rigorous risk assessment when datasets are derived from personal information. By assessing the risks properly and deploying techniques such as anonymisation and pseudonymisation in the right circumstances, organisations may be able to make information derived from personal data available in a form that is rich and usable, whilst protecting individual data subjects rights.

76. In our *Outsourcing Oversight?* report[40], the Commissioner recommended that Government should conduct a comprehensive review of all proactive disclosure provisions regarding contracting, and which affect the public sector. Key recommendations were:

- a review of the publication scheme provisions in FOIA, and relevant provisions in the EIR;
- a review of how these laws complement other procurement laws and Government requirements;
- a consideration of how such provisions are monitored and enforced; and
- an assessment of the available resources.

A wide-ranging review like this would help to make it easier for the public to access information about the performance and delivery of outsourced public services.

77. Our report concluded that, although Contracts Finder had been a response designed to encourage greater involvement of SMEs, it is not seen as the right tool for achieving the end-to-end proactive transparency of contracting data that is needed. It includes the Open Contracting Data Standard only at a basic level and does not include any post-award information.

78. Stakeholders told us that although the Government has some good policies in place and there are also certain legal requirements regarding contract transparency, there is an overreliance on voluntary cooperation, little enforcement or monitoring, and a lack of resources or clear political leadership on transparency.

[40] https://ico.org.uk/media/about-the-ico/documents/2614204/outsourcing-oversight-ico-report-to-parliament.pdf

79. We also heard that Government is hampered by weak information systems, and a confusing landscape of legacy systems that make it impossible to track contract, spend and performance information effectively.

80. Our report said that strengthening FOIA and the EIR would increase access to information on the delivery of public services by organisations outside the public sector. This includes essential and costly public services relating to health and justice. There also needs to be better understanding and promotion of the benefits of transparent data; for example, how it can support the market. This fits with Government policy emphasis on contracts reflecting wider societal values rather than focusing solely on cost.

81. The National Data Strategy provides a welcome opportunity to highlight to the public and promote clear, enforceable and enhanced rights of access to information in an evolving public sector, while also imposing more proactive transparency obligations.

82. Whilst we recommend that organisations include environmental information in their FOIA publication scheme, the EIR instead contain a specific duty to proactively publish environmental information. This may produce environmental benefits around issues such as climate change and biosecurity. The Government might benefit from greater consultation with civil society and the public to inform publication priorities around these aims.

Improving data use – general data sharing and data protection

83. We acknowledge that sharing personal data can bring benefits to everyone. When done in accordance with the law and good practice, data sharing can help the Government and other organisations deliver modern, efficient services and can make everyone's lives easier. Conversely, not sharing data can mean that everyone fails to benefit from these opportunities; and in some instances the chance is missed to assist citizens in need, whether in urgent or longer term situations.

84. It is a legal requirement for controllers to comply with the principles set out in GDPR and set out clearly the personal data rights of individuals and how these will be upheld. If they agree that they are joint controllers under the GDPR, they will have joint responsibility for determining the purpose of and means of personal data processing.[41].

[41] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/

85. In addition, the success of a data sharing initiative depends on a thorough approach, which includes appropriate governance and oversight at both a local and central level. A coordinated cross-Government approach to data sharing would be of advantage to Government departments to ensure that data sharing is undertaken in a coherent and consistent way.

86. But, in doing so, sight should not be lost of the need to consider the proportionality of any planned data sharing, and ensuring appropriate levels of governance, and we recommend this is reflected in the National Data Strategy. The responsibility for accountability will include undertaking robust DPIAs to assess the likely impact of the processing on the rights and freedoms of individuals. Publishing these DPIAs (in a redacted or extracted form, if necessary) assists controllers in complying with the accountability principle.

87. High-level national data sharing protocols might form part of the National Data Strategy to provide a framework for more detailed local data sharing agreements between individual participants. If so, these should be based upon the ICO Data Sharing Code of Practice.

88. The ICO has drafted an updated Data sharing Code of Practice[42] as required under s121 of the DPA and it is currently out for public consultation. It is anticipated that the Code will be laid in Parliament in autumn 2019. The Code will be an essential piece of guidance for organisations involved in data sharing. When published, data controllers should ensure that their processes follow the good practices outlined within it. The National Data Strategy should emphasise the importance of following the Code in any sharing of personal data.

Improving data use - data sharing under the Digital Economy Act 2017

89. Part 5 of the Digital Economy Act 2017(the DEA) introduces a number of new powers to share information to help make the digital delivery of Government services more efficient and effective. We are aware that some data sharing initiatives are operating in, for example, the area of fuel poverty. A number of pilots are being run under the debt and fraud powers, but none of these pilots has yet been recommended to be accepted for 'business as usual'. Even when a pilot is regarded as successful, it will need further legislation

[42] https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

for longer term use. The review boards under the DEA will be reporting on the exercise of powers under the DEA in due course.

90. The DEA also grants the power for public authorities to share information with the UK Statistics Authority. Sharing of data for the purposes of statistics and for research can lead to a better understanding of society and make a valuable contribution to the economy and the development of Government policy. However, public authorities still need to address the principle of proportionality, balancing the benefits of sharing against the risks to the rights of individuals, and ensuring that they comply with the accountability principle under GDPR.

91. The National Audit Office (NAO) report *Challenges in using data across government*[43] refers to Government's consultation with the ICO to ensure that the codes of practice for the DEA comply with GDPR. The NAO report also comments that despite DCMS support to departments on how to use the DEA powers, departments still lack confidence to share data.

Devolved Administrations

92. There are similar data strategies being developed in each of the devolved jurisdictions. Whilst recognising the independence of each, we would encourage complementarity between the strategies to ensure a common level of openness and transparency throughout the UK so no individual is disadvantaged in terms of the information they can access by virtue of their area of residence.

International aspects

93. While the UK remains within the EU, the Commissioner's office represents the UK at the European Data Protection Board (EDPB), the EU body in charge of the application of the GDPR. A key aspect of the EDPB's remit, which contributes to the confidence that individuals can place in data protection measures, is to ensure that data protection law is applied consistently across the EU. The EDPB works to ensure effective cooperation amongst data protection authorities, issuing guidelines on the interpretation of core concepts of the GDPR and ruling by binding decisions on disputes regarding cross-border processing, ensuring a uniform application of EU rules.

[43] https://www.nao.org.uk/wp-content/uploads/2019/06/Challenges-in-using-data-across-government.pdf

94. We also welcome international initiatives such as the Declaration of ethics and data protection in artificial intelligence[44] agreed at the International Conference of Data Protection and Privacy Commissioners 2018, which the Commissioner chairs. Adherence to declarations and protocols such as this can contribute to the trust the public can place in the way that organisations use their data.

95. At the IDPCC 2017[45], a keynote presentation was made by Viljar Peep about the principles behind the sharing of information in the State Portal in Estonia[46]. It appears that there is strong support from the Estonian population for the data sharing and privacy by default has been built in through the use of block chain and encryption.

96. We are aware of initiatives in Canada where progress is being made on an open data agenda. Canada's 2018-2020 National Action Plan on Open Government[47] is a wide-ranging strategy which includes a focus on user-friendly open government and transparency. It also includes expansion of a pilot to allow working documents from government officials to be open by default, subject to restrictions associated with privacy, confidentiality and security.

97. Canada also launched a Data Strategy roadmap for the public service in 2018[48]. Canadian Government departments are now tasked with developing their own data strategies. Also in 2018, the Canadian Ministry of Innovation, Science and Economic Development Canada (ISED), the department responsible for Canadian private sector privacy law (Personal Information Protection and Electronic Documents Act - PIPEDA) released National Digital and Data Consultations[49] to which the Canadian regulator has responded. [50]In May 2019, ISED released a Digital Charter[51]which also included the announcement of discussion papers on PIPEDA and Privacy Act reform.

July 2019

[44] https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf
[45] https://icdppc.org/document-archive/miscellaneous/
[46] https://www.eesti.ee/eng/topics/citizen/riigiportaali_abi/riigiportaali_ajalugu
[47] https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government
[48]https://www.canada.ca/en/privy-council/corporate/clerk/publications/data-strategy.html
[49] https://www.ic.gc.ca/eic/site/084.nsf/eng/home
[50] https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ised_181123/
[51] https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html